R

WIPO
ВСЕМИРНАЯ ОРГАНИЗАЦИЯ
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

WIPO/ACE/18/26 REV.
ОРИГИНАЛ: АНГЛИЙСКИЙ
ДАТА: 15 МАЯ 2026 ГОДА

Консультативный комитет по защите прав

Восемнадцатая сессия
Женева, 2–4 июня 2026 года

УЧАСТИЕ ПОСРЕДНИКОВ В БЛОКИРОВКЕ САЙТОВ: КАК ЗАКОНОДАТЕЛИ, СУДЫ И УЧРЕЖДЕНИЯ ОПРЕДЕЛЯЮТ РОЛЬ ПОСРЕДНИКОВ В БОРЬБЕ С ПИРАТСТВОМ В СФЕРЕ АВТОРСКОГО ПРАВА В ИНТЕРНЕТЕ

Доклад подготовлен г-ном Окке Делфосом Виссером, старшим вице-президентом и заместителем генерального юрисконсульта по международным вопросам Ассоциации кинокомпаний (Motion Picture Association), Брюссель, Бельгия [*]

РЕЗЮМЕ

В данном докладе исследуется важнейшая роль, которую играют посреднические службы, помимо простых поставщиков интернет-услуг (интернет-провайдеры), в блокировании незаконных пиратских сайтов в рамках режимов судебных запретов без установления вины. Современные передовые практики[1], нормативные акты (в частности, Закон о цифровых услугах (DSA) Европейского союза (ЕС)), судебная практика и институциональные правила — все это поддерживает вовлечение широкого круга посредников в процесс блокировки сайтов. В качестве примеров можно привести регистраторов доменных имен, виртуальные частные сети (VPN), поисковые системы и сети доставки контента. Фактически, исследования показывают, что вовлечение широкого круга посредников в процедуры блокировки значительно повышает эффективность мер и снижает количество случаев обхода блокировки. Кроме того, следует использовать автоматизированные решения, согласованные между правообладателями и

[*] Мнения, выраженные в настоящем документе, принадлежат автору и могут не совпадать с мнениями Секретариата или государств — членов ВОИС.
[1] См. материалы Ассоциации кинокомпаний (Motion Picture Association), представленные в ВОИС на семнадцатой сессии Консультативного комитета по защите прав, состоявшейся 4–6 февраля 2025 года, доступные по адресу https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_14_prov.pdf.

соответствующими посредниками, включая интернет-провайдеров, для противодействия множеству тактик обхода блокировки, применяемых сайтами-нарушителями.

I. ЭФФЕКТИВНОСТЬ БЛОКИРОВКИ САЙТОВ

1. Ассоциация кинокомпаний (Motion Picture Association — MPA) выступает в качестве глобального представителя и защитника интересов международной кино-, теле- и стриминговой индустрии[2]. Нашими членами являются Netflix Studios, LLC, Paramount Pictures Corporation, Prime Video & Amazon MGM Studios, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures и Warner Bros. Discovery. MPA играет ведущую роль в борьбе с незаконным распространением контента, защищенного авторским правом, которое наносит ущерб процветающей цифровой экосистеме. Одной из основных целей MPA является сокращение или смягчение последствий пиратства посредством эффективных стратегий правоприменения, в том числе путем сотрудничества с посредниками, которые могут предоставлять онлайн-услуги операторам пиратских ресурсов.

2. Команда MPA по защите контента работает в рамках Альянса за творчество и развлечения (ACE), который является ведущей в мире организацией по борьбе с онлайн-пиратством. ACE был создан в 2017 году по инициативе MPA и в настоящее время объединяет более 50 медиа- и развлекательных компаний по всему миру. ACE уделяет особое внимание правоприменению и сотрудничеству с государственными органами и судебными властями с целью выявления пиратских операторов и организаций, а также закрытия незаконных сервисов. Совместно MPA и ACE применяют комплексный подход к борьбе с онлайн-пиратством, осуществляя широкий спектр мероприятий, таких как сбор разведывательной информации и проведение расследований; мониторинг нового законодательства о блокировке сайтов по всему миру; осуществление действий по получению права на информацию (ROI) для получения данных о пиратских операторах от промежуточных поставщиков услуг; а также подача запросов о блокировке и удалении из списков нарушающих права веб-сайтов или сервисов.

3. В настоящее время в более чем 60 странах действуют правовые системы, допускающие применение административных и/или судебных процедур блокировки сайтов. MPA имеет непосредственный опыт работы в более чем 30 из этих стран и накопила значительный опыт в данной области. Внутренний анализ эффективности распоряжений о блокировке сайтов, полученных в 2024–2025 годах, на основе данных позволил сравнить количество посещений веб-сайтов до и после блокировки. Результаты показывают, что блокировка традиционными ISP приводит к снижению посещаемости целевых пиратских сайтов в среднем на 89%. В таких странах, как Италия, Франция, Бразилия, Южная Корея и Индия, среднее снижение посещаемости после блокировки сайтов в 2024 году превысило 90%[3].

---

[2] https://www.motionpictures.org/about/#mission.

[3] Общедоступные данные также показывают, что эффективность блокировки сайтов колеблется от 60% до 97% в разных странах. Что касается Соединенного Королевства, см. Danaher et al., The Effect of Piracy Website Blocking on Consumer Behavior, MIS Quarterly, 631, июнь 2020 года, стр. 637 и 639 («блокировка [53 сайтов] в ноябре 2014 года оказалась эффективной в плане сокращения посещений заблокированных сайтов. Число посещений заблокированных сайтов сократилось на 88% за период от трех месяцев до блокировки до трех месяцев после нее». Со ссылкой на данные о волнах блокировок в 2012 и 2013 годах: «число посещений заблокированных сайтов сокращается на 80–95% в различных группах, что свидетельствует об эффективности блокировки»), по адресу https://www.cmu.edu/entertainment-analytics/documents/effectiveness-of-anti-piracy-efforts/uk-blocking-misq.pdf. Что касается Австралии и Южной Кореи, см. MPA, Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior январь 2020 года, доступно по адресу https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf (ссылаясь на блокировку в декабре 2018 года: «средняя посещаемость заблокированных сайтов резко

4. Эффективность блокировки сайтов также оценивалась с точки зрения роста легального потребления в Бразилии, Индии, Соединенном Королевстве и Австралии. Несколько исследований показали, что блокировка сайтов способствовала росту легального потребления на 5,2% в Бразилии в 2021 году и на 8,1% и 3,1% в Индии в 2019 и 2020 годах соответственно[4]. Проведенное в 2020 году в Соединенном Королевстве исследование показало, что благодаря блокировке сайтов использование легальных сайтов по подписке увеличилось на 7–12 процентных пунктов[5]. Наконец, в Австралии трафик на сайты легального просмотра контента вырос на 5%[6].

5. Правообладатели вкладывают огромные средства в контент, а их доходы и перспективы будущего производства серьезно страдают от пиратства. Для дальнейшего повышения эффективности блокировки доступа к пиратскому контенту необходимо вмешательство и сотрудничество поставщиков посреднических онлайн-услуг на всех этапах цепочки незаконного распространения. Эту необходимость признает все большее число законодателей, судов и административных органов.

II. ЗАКОН О ЦИФРОВЫХ УСЛУГАХ (DSA) СЛЕДУЕТ ПО СТОПАМ ДИРЕКТИВЫ ЕС ОБ ЭЛЕКТРОННОЙ КОММЕРЦИИ

6. Закон о цифровых услугах (Постановление ЕС № 2022/2065)[7] является одним из наиболее всеобъемлющих законодательных актов, регулирующих ответственность онлайн-посредников, и имеет прямое применение во всех 27 государствах — членах ЕС. Опираясь на Директиву ЕС об электронной коммерции и повторяя большинство ее статей, DSA унаследовал те же правила «безопасной гавани» для простых каналов передачи данных, провайдеров кэширования и хостинга, но также дополнительно уточнил, какие посредники должны подпадать под эти соответствующие категории.

7. В этом отношении пункт 29 преамбулы[8] Закона о цифровых услугах (DSA) чрезвычайно полезна для уточнения того, какие посредники подпадают под определение

снизилась в экспериментальной группе, причем посещаемость этой группы сайтов снизилась в целом на 61% в период после блокировки по сравнению с периодом до нее»), а также MPA, MPA Study on Site Blocking Impact in South Korea, 2016 год, стр. 11, доступно по адресу https://www.mpa-apac.org/wp-content/uploads/2018/05/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf («последствия уровня 1 были очевидны: посещаемость заблокированных сайтов снизилась в среднем на 90% через три месяца после блокировки (на 97% после первой волны, на 93% после второй волны и на 79% после третьей волны)»).

[4] См. Danaher et al., The Impact of Online Piracy Website Blocking on Legal Media Consumption, 12 февраля 2024 года, доступно по адресу https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522.

[5] См. Danaher et al., The Effect of Piracy Website Blocking on Consumer Behavior, MIS Quarterly, 631, июнь 2020 года, указанную выше.

[6] См. Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior, указанную в сноске 3.

[7] Текст Закона о цифровых услугах (DSA) доступен по адресу https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

[8] В пункте 29 преамбулы к Закону о цифровых услугах (DSA) указано, что «услуги посредников охватывают широкий спектр видов экономической деятельности, осуществляемой в сети Интернет, и постоянно развиваются с целью обеспечения быстрой, надежной и безопасной передачи информации, а также удобства для всех участников онлайн-экосистемы». Например, посреднические услуги типа «простого канала» включают общие категории услуг, такие как точки обмена интернет-трафиком, точки беспроводного доступа, виртуальные частные сети, услуги системы доменных имен и резолверы, реестры доменных имен верхнего уровня, регистраторы, центры сертификации, выдающие цифровые сертификаты, услуги передачи голоса по ИС и другие услуги межличностной связи, в то время как общие примеры посреднических услуг типа «кеширования» включают исключительно предоставление сетей доставки контента, обратных прокси-серверов или прокси-серверов адаптации контента. Такие услуги имеют решающее значение для обеспечения бесперебойной и эффективной передачи информации в интернете. Примерами «услуг хостинга» являются такие категории услуг, как облачные вычисления, веб-хостинг, платные услуги по поисковой оптимизации или услуги, позволяющие обмениваться информацией и контентом в сети, включая хранение и обмен файлами. Посреднические услуги могут предоставляться изолированно, как часть другого вида посреднической услуги или одновременно с другими посредническими услугами. То, является ли конкретная услуга услугой «простого канала», «кеширования» или «хостинга», зависит исключительно от ее технических функций, которые могут меняться со временем, и должно оцениваться в каждом конкретном случае.

провайдеров «простых каналов», включая VPN, системы доменных имен (DNS), резолверы и регистраторов, в то время как приведенные примеры провайдеров «кеширования» включают сети доставки контента (CDN) и обратные прокси.[9]

8. Кроме того, в пункте 25 преамбулы[10] подчеркивается важность обеспечения того, чтобы судебные запреты без установления вины распространялись на посредников, которые, хотя и не несут ответственности, тем не менее обладают технической возможностью вмешаться и прекратить или предотвратить нарушение, в том числе путем блокирования доступа к конкретному незаконному контенту.

9. Наконец, пункт 31 преамбулы[11] предусматривает, что государства-члены могут выбрать судебную и/или административную процедуру для получения таких судебных приказов, что прямо предусмотрено статьями 4–6. Правовая основа для таких видов судебных приказов содержится в прежней статье 8(3) Директивы 2001/29/ЕС Европейского парламента и Совета, которая прямо упоминала подобные меры в отношении посредников для защиты авторских прав.[12]

10. Следует отметить, что эта правовая инфраструктура не является беспрецедентным изобретением ЕС и не применяется только там, как подчеркивается ниже в связи с индийской судебной практикой. Фактически она вытекает из статьи 14(2) Договора Всемирной организации интеллектуальной собственности (ВОИС) об авторском праве 1996 года[13], касающегося защиты авторских и смежных прав в цифровой среде, который обязывает договаривающиеся Стороны обеспечить наличие в их законодательстве

---

[9] Европейские суды уже ссылаются на DSA для расширения сферы применения судебных запретов без установления вины на другие виды посредников с целью защиты произведений, охраняемых авторским правом, например, Гражданский суд Парижа, который в своем решении от 28 марта 2025 года по делу Canal Plus против Cloudflare Inc. указал, что «Поставщики систем разрешения доменных имен и сетей доставки контента, которые прямо охватываются вышеупомянутым Постановлением DSA, несмотря на любые исключения из ответственности, которыми они могут в иных случаях пользоваться, выполняют функцию передачи».

[10] В пункте 25 преамбулы DSA указано, что «Исключения из ответственности, установленные в настоящем Регламенте, не должны влиять на возможность вынесения различных видов судебных запретов в отношении поставщиков посреднических услуг, даже если они соответствуют условиям, изложенным в рамках этих исключений». Такие судебные запреты могут, в частности, состоять из постановлений судов или административных органов, вынесенных в соответствии с законодательством Союза, требующих прекращения или предотвращения любого нарушения, включая удаление незаконного контента, указанного в таких постановлениях, или блокировку доступа к нему».

[11] В пункте 31 преамбулы DSA предусмотрено, что «в зависимости от правовой системы каждого государства-члена и рассматриваемой области права национальные судебные или административные органы, включая правоохранительные органы, могут предписывать поставщикам посреднических услуг принять меры в отношении одного или нескольких конкретных элементов незаконного контента или предоставить определенную конкретную информацию. Национальные законы, на основании которых издаются такие предписания, значительно различаются, и все чаще такие предписания касаются трансграничных ситуаций. Для обеспечения эффективного и действенного выполнения таких распоряжений, в частности в трансграничном контексте, с тем чтобы соответствующие государственные органы могли выполнять свои задачи, а поставщики не несли несоразмерного бремени, без неоправданного ущемления прав и законных интересов третьих лиц, необходимо установить определенные условия, которым должны соответствовать такие распоряжения, а также определенные дополнительные требования, касающиеся их выполнения. Следовательно, настоящее Постановление должно гармонизировать лишь определенные конкретные минимальные условия, которым должны соответствовать такие постановления, чтобы возникло обязательство поставщиков посреднических услуг информировать соответствующие органы о мерах, принятых во исполнение этих постановлений. Таким образом, настоящее Постановление не создает правовую основу для выдачи таких постановлений и не регулирует их территориальный охват или трансграничное исполнение.

[12] Статья 8(3) Директивы 2001/29/ЕС гласит, что «государства-члены должны обеспечить, чтобы правообладатели имели возможность подавать заявления о вынесении судебного запрета в отношении посредников, услуги которых используются третьими лицами для нарушения авторского права или смежных прав».

[13] Текст Договора ВОИС об авторском праве (ДАП) доступен по адресу https://www.wipo.int/wipolex/en/text/295166.

процедур правоприменения, позволяющих принимать эффективные меры против любого акта нарушения прав, охватываемого Договором, включая оперативные меры правовой защиты для предотвращения нарушений и меры, служащие сдерживающим фактором для дальнейших нарушений.

III. УЧАСТИЕ ДРУГИХ ВИДОВ ПОСРЕДНИКОВ НА ПРАКТИКЕ

11. В современную эпоху технологий пиратский контент в основном потребляется в Интернете. С начала 2000-х годов рост числа благоприятных судебных прецедентов позволил правообладателям добиваться вынесения судебных запретов без установления вины, которые сначала носили статический характер, а впоследствии стали динамическими, обязывая интернет-провайдеров блокировать доступ к пиратским сайтам и сервисам. В тех случаях, когда соответствующая информация была доступна, правоприменение было направлено непосредственно на операторов пиратских ресурсов и хостинг-провайдеров. Однако практический опыт показывает, что операторы часто скрываются за вымышленными или похищенными личностями и не выполняют предписания о прекращении деятельности. Между тем хостинг-серверы зачастую невозможно отследить, поскольку они защищены методами анонимизации или расположены в странах, где правоприменение чрезвычайно затруднено.

12. Сотрудничество со всеми посредниками в цепочке пиратства имеет решающее значение, поскольку каждый из них может эффективно вмешиваться в пределах своей компетенции и применять наиболее подходящие меры. Такой подход повышает эффективность и расширяет охват распоряжений о блокировке, одновременно сокращая возможности обхода. К ключевым посредникам относятся поисковые системы, регистраторы доменов, сети доставки контента, VPN и альтернативные системы доменных имен.

A. Приостановка действия домена и ее эффективность

13. Регистраторы доменных имен (DNR) регистрируют доменные имена за плату от имени регистрантов, т. е. владельцев веб-сайтов, чтобы буквенно-цифровой IP-адрес, используемый для домена, можно было легко найти с помощью поисковых систем.

14. Недавно, в соответствии с судебными предписаниями, DNR приостановили работу незаконных доменов с глобальным эффектом, сделав множество целей недоступными со всего мира. С 2023 года[14] Высокий суд Дели в Индии выносит постановления, обязывающие DNR, независимо от их местонахождения, блокировать и приостанавливать работу нарушающих права доменных имен. В 2025 году судебные запреты были распространены на нарушающие права приложения и другие сервисы, защищая трансляции в реальном времени[15]. В постановлении, вынесенном в пользу Star India от 29 мая 2025 года, Высокий суд Дели заявил следующее:

> «В новую эру технологий сегодня нарушителям стало все легче и удобнее создавать буквенно-цифровые/зеркальные/перенаправляющие варианты нарушающих права веб-сайтов, и к моменту, когда может произойти привлечение к делу третьих лиц и расширение мер правовой защиты, определенные чувствительные ко времени нарушающие права действия, такие как прямая трансляция спортивных событий, уже начались незаконно, и к тому моменту, когда

[14] См. дело Universal City Studios LLC. и др. против Dotmovies.baby и др., CS(COMM) 514/2023.
[15] См. дело Star India Private Limited против IPTV Smarters, дело № CS(COMM) 108/2025, 29 мая 2025 года. См. также дело Dazn Limited & Anr против Buffsports. Me & Ors., CS(COMM) 536/2025, 28 мая 2025 года.

пострадавшая сторона, такая как истец, обращается в этот суд, уже слишком поздно», поручив регистраторам «приостанавливать регистрацию доменных имен нарушающих прав доменов/URL-адресов/пользовательских интерфейсов, о которых уведомляет истец, в режиме реального времени».

15. В результате несколько регистраторов по всему миру выполнили эти судебные постановления, приостановив домены по всему миру и предоставив информацию об операторах пиратских ресурсов[16]. Однако некоторые регистраторы по-прежнему не выполняют судебные постановления, что подчеркивает необходимость более тесного сотрудничества и большего осознания их важной роли.

16. Внутренний анализ 275 популярных пиратских сайтов, заблокированных в Индии, показал, что[17] в течение трех месяцев до и трех месяцев после вынесения судебных решений количество посещений 138 доменов, которые были заблокированы и приостановлены, сократилось еще на 11% по сравнению с посещениями остальных 137 доменов, заблокированных только на местном уровне интернет-провайдерами. Глобальный эффект оказался еще более выраженным: количество посещений доменов, которые были заблокированы также в других странах и приостановлены регистраторами, сократилось в среднем на 44% больше, чем у тех, которые были заблокированы только локально. В целом, с июля 2024 года по июль 2025 года количество посещений заблокированных и приостановленных сайтов по всему миру сократилось на 99%, поскольку приостановка домена, как правило, делает его недоступным для любых способов обхода блокировки сайтов, таких как использование VPN и альтернативных систем доменных имен[18].

B. Блокировка сетей доставки контента

17. В цепочке распространения пиратского контента различные незаконные сервисы также используют обратные прокси-серверы и услуги CDN[19]. Достигнут определенный прогресс, включая специальные интерфейсы прикладного программирования (API) для правообладателей, позволяющие запрашивать более подробную информацию о доменах, скрывающих свой реальный IP-адрес за обратными прокси-серверами; льготное отношение к так называемым «надежным заявителям»; а также технологические меры по блокированию доступа к незаконному контенту на уровне CDN[20].

---

[16] В решении по делу Star India против IPTV Smarters суд обязал ответчиков «раскрыть полную информацию, такую как имя и адрес, а также платежные реквизиты, относящиеся к указанным недобросовестным веб-сайтам и мобильным приложениям».

[17] «Популярный домен» — это веб-сайт, который в месяц приостановки получил более 50 000 посещений со всего мира.

[18] Хотя можно ожидать, что приостановленные и заблокированные домены станут полностью недоступными (снижение посещаемости на 100%), различия в измеренном снижении могут быть связаны с неточностью в сообщении дат вступления в силу приостановки домена, а также с остаточными посещениями по старым ссылкам.

[19] См. отчеты ЕС о списках объектов наблюдения в связи с контрафактом и пиратством за 2025 и 2022 годы. Доступны по адресу https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2025)132&lang=en; и https://circabc.europa.eu/ui/group/d0803128-7d62-40ee-8349-c43ee92745aa/library/b36f701d-2850-4768-9b3e-e487140e11e5/details?download=true.

[20] Испанская LaLiga неоднократно подтверждала, что достигла соглашений с Akamai Technologies и CDN77 об удалении контента, нарушающего авторские права, даже в режиме реального времени. См. https://www.panoramaaudiovisual.com/2025/04/04/laliga-trabaja-cdn77-akamai-lucha-contra-pirateria/. См. также решение Парижского гражданского суда от 28 марта 2025 года, упомянутое выше. Кроме того, компания Cloudflare заявила, что на основе добровольных соглашений с правообладателями возможна геоблокировка веб-сайтов с помощью ее CDN и служб безопасности, как это было сделано в Соединенном Королевстве. См. новость в блоге Cloudflare здесь https://blog.cloudflare.com/h1-2025-transparency-report/.

18. Строгое обеспечение соблюдения блокировок доступа к CDN могло бы существенно сократить посещаемость пиратских сайтов, однако остаются значительные проблемы. Главная из них — способность операторов пиратских сайтов регистрировать практически бесконечное количество доменов на своих учетных записях CDN и легко управлять ими, так что, как только текущий домен блокируется, его заменяет новый домен, который сразу же готов к работе.

C. Своевременное исключение из списков поисковых систем

19. Исключение из списков результатов поиска означает удаление конкретных веб-страниц или ссылок из результатов поисковых систем, с тем чтобы они больше не отображались в поисковом индексе при выполнении запросов. Австралия первой включила в свой Закон об авторском праве обязательные положения о «поставщиках услуг онлайн-поиска» и судебных запретах на индексацию, что привело к заключению добровольных соглашений с ведущими поисковыми системами, которые теперь применяют эту практику в различных странах. Другим примером является решение Верховного суда Франции по делу Allostreaming[21], в котором суд обязал поставщиков услуг поиска исключить из индекса веб-сайты, систематически нарушающие авторские права, в соответствии с практикой осуществления Францией статьи 8(3) Директивы об информационном обществе.

20. В сочетании с блокировкой сайтов удаление из списков поисковых систем оказывает значительное влияние на сокращение общего числа посещений недобросовестных веб-сайтов. Внутренние исследования показывают, что своевременное удаление из списков, осуществляемое вскоре после локальной блокировки интернет-провайдерами, приводит к снижению трафика в среднем на 25% больше, чем в случаях, когда своевременное удаление из списков не проводилось.

21. Если названия пиратских сайтов (пиратских брендов) и последние активные домены по-прежнему остаются в верхней части результатов поисковых систем, интернет-пользователям всегда будет относительно легко их найти, независимо от любых предыдущих блокировок. По этой причине своевременное и добросовестное сотрудничество и меры, принимаемые поисковыми системами, остаются крайне важными.

D. VPN и альтернативная блокировка системы доменных имен для предотвращения тактик обхода

22. VPN и альтернативные системы доменных имен — это посредники, которые могут обеспечить доступ к доменам, заблокированным местными интернет-провайдерами. Хотя их можно использовать на законных основаниях в целях обеспечения конфиденциальности, они все чаще применяются в качестве средств обхода ограничений. Недавно законодательство и судебная практика Франции и Италии включили такие типы посредников в сферу действия своих режимов блокировки сайтов.

---

[21] См. решение Верховного суда Франции от 6 июля 2017 года, ECLI:FR:CCASS:2017:C100909. Google, Microsoft Bing и Yahoo! были обязаны исключить из списка сайты, систематически нарушающие авторские права, в соответствии с практикой осуществления Францией статьи 8(3) Директивы 2001/29/EC, позволяющей правообладателям запрашивать соразмерные меры в отношении любого лица, которое может способствовать устранению нарушений. Согласно прецедентному праву по делу Allostreaming, от интернет-провайдеров и поисковых систем может потребоваться полное покрытие расходов на эти меры при условии, что судебный приказ оставляет посреднику свободу определять фактические меры, необходимые для достижения целевого результата, и не требует «невыносимой жертвы».

23. В Италии действующая версия закона о борьбе с пиратством[22] включает оба типа посредников в число тех, на которых могут распространяться предписания, налагаемые национальным органом по телекоммуникациям (AGCOM)[23]. Во Франции в период с 2024 по 2025 год Парижский гражданский суд вынес несколько постановлений о блокировке сайтов в отношении известных VPN-сервисов и альтернативных систем доменных имен[24]. Суд постановил, что эти посредники могут способствовать устранению нарушений благодаря своей деятельности по передаче данных, в том числе в соответствии с положениями DSA, которые квалифицируют их как посреднические услуги. В соответствии с судебной практикой Суда Европейского союза[25] эти меры были признаны соразмерными, поскольку они были ограничены по времени и оставляли посредникам свободу выбора наиболее подходящих технических средств, не налагая на них общей обязанности мониторинга.

IV. ГИБКИЕ СУДЕБНЫЕ ПОСТАНОВЛЕНИЯ ДЛЯ БОРЬБЫ С МЕНЯЮЩИМИСЯ СТРУКТУРАМИ ПИРАТСТВА

24. Недавние события в Соединенном Королевстве иллюстрируют, как суды адаптируют рамки судебных запретов для борьбы с меняющимся характером онлайн-пиратства. Опираясь на давнюю британскую судебную практику по блокировке сайтов в соответствии со статьей 97A Закона об авторском праве, промышленных образцах и патентах, включая традиционные постановления о блокировке сайтов и последующие постановления о блокировке пиратских брендов, Высокий суд справедливости вынес более широкое «сводное» постановление о блокировке сайтов[26].

25. Данное постановление позволяет правообладателям добиваться блокировки структурно нарушающих авторские права аудиовизуальных пиратских сервисов, отвечающих определенным критериям, без необходимости подавать новое судебное ходатайство в отношении каждого нового домена или названия сайта, которые появятся в будущем. Это особенно важно в тех случаях, когда операторы пиратских ресурсов используют общие, описательные или часто меняющиеся названия, чтобы избежать

---

[22] Закон № 93/2023.

[23] Например, Google, по-видимому, добился значительного прогресса в сотрудничестве по блокировке в режиме реального времени на уровне системы доменных имен (см. публичное заявление AGCOM о сотрудничестве с Google, доступное по адресу https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-39), в то время как сотрудничество с провайдерами VPN представляется менее неочевидным, учитывая, что провайдеры VPN, по-видимому, крайне неохотно идут на сотрудничество.

[24] Что касается VPN, см. решения по следующим делам Парижского гражданского суда: № 24/14722 от 15 мая 2025 года и № 25/05198 от 18 июля 2025 года, в обоих из которых фигурировали компании Canal + против Express Technologies, Expressco Services, Cyberghost, Proton, NordVPN и Surfshark. Альтернативные системы доменных имен фигурировали в следующих решениях Парижского гражданского суда: № 23/14722 и № 23/14726 от 16 мая 2024 года, № 23/14731 от 30 мая 2024 года, № 24/06759 от 12 сентября 2024 года, № 24/11187 и № 24/11188 от 24 октября 2024 года, Canal + против Google, Cloudflare и Cisco, № 24/12413, № 24/12414 от 5 декабря 2024 года, Canal + против Vercara LLC и Quad9, и № 24/12415 от 5 декабря 2024 года, Canal + против Google, Cloudflare и Vercara. Эти иски были поданы на основании широкого определения, содержащегося в статье 333-10 Французского спортивного кодекса, о «любом лице, которое может способствовать устранению» нарушения прав на аудиовизуальную эксплуатацию, что позволяет включить в эту категорию VPN и альтернативные системы доменных имен. Суд обязал альтернативных провайдеров системы доменных имен реализовать в рамках своих соответствующих услуг по разрешению доменных имен «все надлежащие меры блокировки для предотвращения доступа с территории Франции, любыми эффективными средствами, и в частности путем блокировки доменных имен или поддоменов, к идентифицированным веб-сайтам».

[25] См. решение Суда Европейского Союза по делу C-314/12 от 24 марта 2014 года, UPC Telekabel Wien GmbH против Constantin Film Verleih GmbH.

[26] См. решение Высокого суда [2026] EWHC 1087 (Ch) от 7 мая 2026 года по делу Columbia Pictures Industries, Inc. и др. против British Telecommunications Plc и др.

попадания под действие постановлений, основанных на брендах или конкретных доменах.

26. Суд признал, что такая более широкая форма правовой защиты является необходимой и соразмерной с учетом масштабов и динамичного характера проблемы онлайн-нарушений, операционной нагрузки, связанной с повторными заявлениями, а также продемонстрированного на протяжении многих лет ответственного использования правообладателями мер по блокировке сайтов. Постановление действует в течение 6 месяцев и может быть продлено в зависимости от обязательства по представлению отчетности ex-post, требующего от правообладателей представления суду информации о выполнении и эффективности, что позволяет сохранить судебный надзор и подотчетность. Данный тип постановления не требует расширения ответственности посредников, а скорее обеспечивает сохранение практической эффективности существующих механизмов судебных запретов без установления вины в быстро меняющихся онлайн-условиях.

27. Это особенно актуально в свете недавних изменений в техническом и операционном поведении пиратских операторов. Хотя пока не известно о широком использовании полностью автономных систем «агентного ИИ» в экосистеме пиратства, ряд технологических разработок уже существенно снижает барьеры для крупномасштабного переключения доменов и обходных схем, так что операторы пиратских ресурсов теперь могут быстро развертывать клонированные сайты потокового вещания, используя общедоступные кодовые базы и недорогие автоматизированные системы регистрации доменов, часто в сочетании с API массовой регистрации и стратегиями миграции на основе перенаправления. В результате, услуги, нарушающие авторские права, все чаще работают через сменяющие друг друга сети доменов, включая общие или не связанные с брендами имена, специально разработанные для обхода традиционных мер блокировки, ориентированных на конкретные домены или бренды. В некоторых случаях операторы поддерживают несколько взаимозаменяемых доменов с практически идентичной инфраструктурой, библиотеками контента и функциональностью, что позволяет беспрепятственно перенаправлять пользователей на запасные домены.

V. Автоматизация

28. Еще одним явлением, набирающим обороты, является внедрение автоматизированных платформ, не только для лучшей координации запросов правообладателей, но и для привлечения самых разнообразных посреднических сервисов к их деятельности по блокировке. Такие платформы могут работать в соответствии с передовой практикой, соблюдая надлежащую процедуру, принципы прозрачности и соразмерности, а также процессуальные гарантии, обеспечивая прямое общение правообладателей с посредниками, как под надзором третьей стороны, так и без него.

29. Такой автоматизированный подход сделал бы сотрудничество между сторонами более плавным и экономически эффективным, позволяя осуществлять быструю блокировку и разблокировку, что также подходит для согласования необходимости защиты от незаконной передачи контента в режиме реального времени. Поэтому следует поощрять внедрение таких систем, заменяющих обмен электронными письмами с вложениями, которые обычно требуют более длительного времени обработки и сопряжены с большей сложностью.

30. Некоторые национальные административные органы[27] уже оснастили себя автоматизированными или полуавтоматизированными платформами, которые постоянно совершенствуются и позволяют осуществлять быструю блокировку и разблокировку, а также обеспечивают беспрепятственную коммуникацию между правообладателями, посредниками и надзорными органами. Суды, по-видимому, поощряют использование автоматизированных средств обновления и уведомления между правообладателями и посредниками[28]. Однако частные организации, такие как MPA, также оснащают себя аналогичными инструментами, которые облегчают выявление нарушений, сбор доказательств и коммуникацию с посредниками.

VI. ЗАКЛЮЧЕНИЕ

31. Эмпирические данные показывают, что более тесное сотрудничество различных посредников в деле предотвращения доступа к незаконным сайтам и услугам приводит к более эффективной блокировке и более надежной защите интеллектуальной собственности.

32. Следует более активно использовать средства автоматизации и технологические инструменты для борьбы с пиратством с целью повышения эффективности и обеспечения большей согласованности с системами посредников, что в долгосрочной перспективе позволит сократить расходы и снизить нагрузку. Такой подход поможет бороться с пиратством и его будущими проявлениями, защищая как правообладателей, так и, в конечном счете, самих пользователей, которые подвергаются риску заражения вредоносным ПО и кражи личных данных на пиратских веб-сайтах.

[Конец доклада]

[27] Известными примерами являются AGCOM в Италии, Греческая организация по авторскому праву (EDPPI) в Греции, Генеральная инспекция культурной деятельности (IGAC) в Португалии и Национальный орган по телекоммуникациям (ANATEL) в Бразилии.
[28] См. решение Федерального суда по гражданским и коммерческим делам Аргентины (11-я палата) от 7 апреля 2025 года, № 4426/2025, по делу Warner Bros. Entertainment Inc. и др. против Pelisplushd.bz и др.